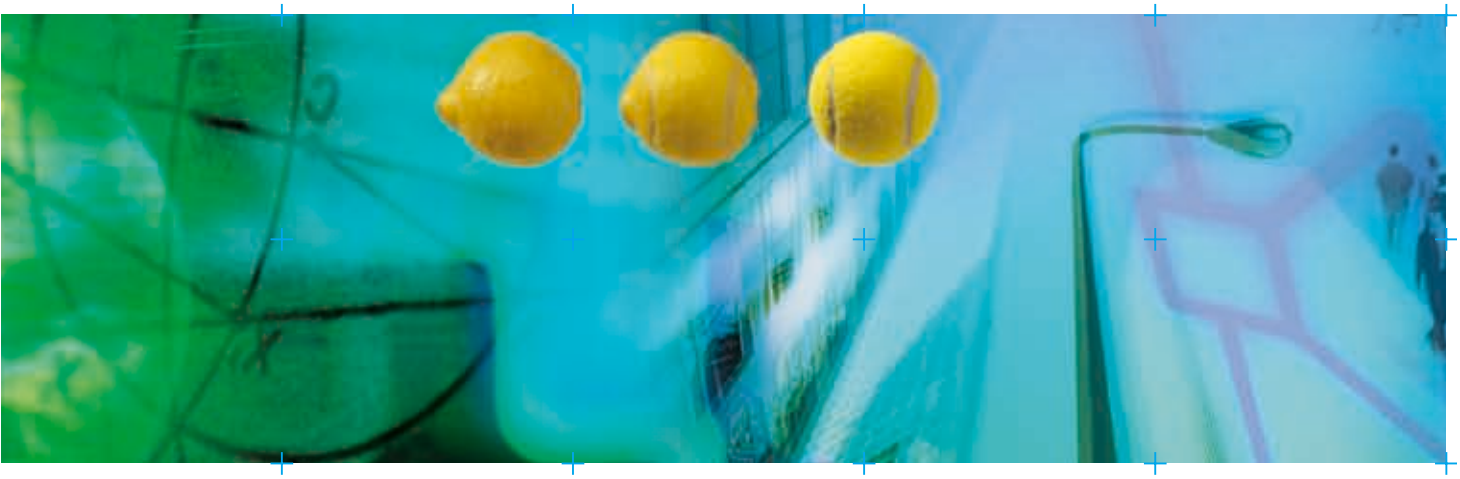
PRISE privacy security

Norske holdninger til sikkerhetsteknologier og personvern

Rapport fra møte med norske innbyggere

Teknologirådet



Rapport 4 – 2007

Norske holdninger til sikkerhetsteknologier og personvern

Rapport fra møte med norske innbyggere

PASR – Preparatory Action on the enhancement of the European industrial potential in the field of Security research

Grant Agreement no. 108600

Supporting activity acronym: PRISE
Activity full name: Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies

ISBN 978-82-92-44716-1

Utgitt: Oslo, oktober 2007
Omslag: Enzo Finger Design AS
Layout: Sissel Sandve / Basta
Trykk: ILAS Grafisk

Elektronisk publisert på: www.teknologiradet.no

Contents

Forord

Forholdet mellom samfunnets sikkerhet og den enkeltes personvern er et viktig tema i samfunnsdebatten. Nye sikkerhetsteknologier sammen med nye behov for kontroll og overvåkning gjør at det samlede nivået av overvåkning i samfunnet er stadig stigende.

Dette dokumentet inngår som en del av PRISE-prosjektet (PRIvacy and Security in Europe). Siktemålet med prosjektet er å bidra til en sikker fremtid for Europa i tråd med europeiske borgeres rettigheter og preferanser, og da særlig retten til personvern. Prosjektet gjennomføres i samarbeid med institusjoner i Danmark (Teknologirådet), Tyskland (Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein) og Østerrike (Institut für Technikfolgen-abschätzung, ITA). Prosjektet er støttet av EU og resultatene vil bli presentert for EU-kommisjonen.

En viktig del av PRISE-prosjektet har vært at vanlige innbyggere, uten spesielle forkunnskaper, har uttalt seg om hvordan samfunnet bør håndtere balansen mellom sikkerhet og personvern. I mai/juni 2007 ble innbyggere i seks europeiske land; Norge, Danmark, Tyskland, Østerrike, Spania og Ungarn invitert til nasjonale intervjumøter.

Dette er rapporten fra det norske møtet. Der ble det drøftet fremtidsbilder, tatt stilling til konkrete dilemmaer og gitt anbefalinger til hva man mener er viktig ved utvikling og implementering av nye sikkerhetsteknologier. Prosjektet skal bruke resultatene til å utarbeide kriterier for utvikling og implementering av nye sikkerhetsteknologier.

Teknologirådet har også utgitt synteserapporten, «Europeiske holdninger til sikkerhetsteknologier og personvern», samt rapportene «Oversikt over sikkerhetsteknologier» og «Scenarier» fra PRISE-prosjektet.

Jeg vil benytte anledningen til å takke alle deltakerne på det norske møtet i Sandnes for å sette av tid til å komme med sine verdifulle vurderinger. Takk også til prosjektleder Åse Kari Haugeto fra Teknologirådet.

Tore Tennøe
Sekretariatsleder, Teknologirådet

Introduction

This report sums up the Norwegian «interview meeting» about privacy and security technologies that was arranged as a part of the PRISE-project. PRISE is financed by the European Commission, and will provide guidelines and support for the development of security solutions with a particular emphasis on human rights, human behaviour and people's perception of security and privacy. The interview meetings are a central element in the PRISE-project. Interview meetings were subsequently held in Denmark, Norway, Germany, Austria, Spain and Hungary.

The planning, execution and reporting of the Norwegian interview meeting, have all been done by the secretariat of the Norwegian Board of Technology (NBT).

The interview meeting was arranged on the 4th of June 2007 in the town Sandnes, located in Rogaland, at the south west coast of Norway.

26 laypeople participated in the interview meeting. The participants heard a presentation, filled out a questionnaire and debated issues of new security technologies and protection
of privacy (A2).

Choosing Participants for the Meeting
Recruitment was done by sending letters of invitation to 2000 persons living in 5 municipalities in Rogaland, included the municipality of Stavanger, the metropolis in the area. The 2000 persons were randomly selected, but with criteria of even distribution between sexes, ages between 18-80 years, and geographical location (with correlation between the number of participants invited from each municipality and the population of that municipality).

A total of 31 people applied for participating in the meeting and 26 of them showed up. The five people who were absent contacted us in advance, stating reasons of time constraints (2) and illness (3).
The group of 26 was a good representation of the people living in the area (A1). The participants were between 17-60 years old, with a bit higher representation of those between 35-54 years. The gender distribution was almost equal, and so was the level of education (a slight overweight of people with higher education). Most of the participants were living in the metropolitan area of Stavanger, and only a few were living on the countryside. All participants were familiar with use of mobile phones, e-mail and Internet. Most of them used these technologies daily. The participants reported to travel mainly by car, only seldom traveling by public transport. An exception was the frequency of going by plane, which was rather high for the majority of the participants.

Arranging the Meeting
The interview meeting was prepared and arranged in accordance with the project manual.

The interview meeting was held after working hours, and took place in a municipal training centre in the town centre of Sandnes. Six persons from the staff of NBT were present; the director Tore Tennøe, technology and security expert Christine Hafskjold, and 4 interviewers; Jon Fixdal, Kari Laumann, Jon Magnar Haugen and Åse Kari Haugeto. In addition a photographer was hired to document parts of the meeting, and there were representatives from one local and one national newspaper present.

There were no plenum discussions, but between sessions there were a lot of engaged discussions among the participants, and between participants and the journalists present. Many participants expressed a need for more public debate on the topic. NBT encouraged the participants to keep the discussion going after having left the meeting.

Headline News Prior to the Meeting

There were a couple of relevant news stories in the media just before the meeting. These were referred to by participants during the meeting. One story focused on disloyal attendants in banks having sold information about the royal family's use of credit cards to the tabloid press. Another news story entailed a woman being killed by her ex-boyfriend although her personal protection alarm connected to the police was activated. Because of technical problems, the police went to the wrong location, and the tragedy was complete. Moreover, there was extensive news coverage on Facebook at the time. Facebook, a web based network community, grew extremely rapidly in Norway in the first months of 2007. Three out of four discussion groups at the interview meeting touched on Facebook.

Executive Summary

Security and privacy are complex topics, covering a multitude of uncertainties and ethical dilemmas. Within the group of 26 participants various viewpoints were expressed, and it was clear that the participants had different attitudes towards what is acceptable use of security technologies and what is not.

First, it was evident that there was not a common understanding about what threats are present in our society. Even though most of the participants accepted that there is a threat of possible terrorist attacks in the aviation in Norway, particularly at international flights, many of them stated that this is not by far the most important threat we have to deal with these days. Many, but not all of the participants, questioned if there is an actual terrorist threat at all. Data crime was another topic that was of grave concern to some of the participants. However, it was mainly referred to as the danger of non-authorized personnel and criminals access information. Misuse by authorized personnel, governmental systems etc., was not emphasized as an important threat. This indicates that Norwegians have a strong trust in authorities. Many of the participants stated that perhaps it is not necessary to implement the same security level in Norway as other countries because Norway is looked upon as a «different» society, small and transparent as it is.

The question of what constitutes violation of privacy was reflected on during the interviews, and there were a broad range of interpretations. Participants expressed that both their personal and others' attitudes are changing. Technological development that results in new practices and possibilities seems to change people's tolerance and preferences. The main development is in the direction of people allowing more of their privacy to be exposed for convenience or security reasons. But the major part of the participants was critical to commercial interests' infringement on their privacy.

Some technologies received more attention than others. The automatic speed control by the e-Call system and the «naked machine» were discussed thoroughly. Participants expressed a general mistrust towards all kinds of location technologies (mobile phones, cars etc.), as well as surveillance of the body (cameras in fitting rooms etc.). The response indicated that the use of technologies that is familiar is more accepted than the use of new technologies or new patterns (at new places, by new purposes etc.). This phenomenon could be worth a study in it self; how adaptable society is to new technology, and how this can be used or abused to change society.

Finally, the majority of the participants regarded public information, open discussions and reflections as crucial for the ability to decide what kind of future society we want. Because of the speed of technological development, participants expressed fear that societal consequences would not be properly evaluated. By involving a broad range of citizens at an early stage, most of the participants believed that development can be directed towards a commonly preferred future.

Chapter 1 | General Attitudes

The participants' general attitude to security technologies varied quite a lot. There were those who stated that they did not at all understand the problem by being under surveillance;

«Personally I want it to be a lot of surveillance! (...) I really can't understand why people fear being surveilled in their own country if they didn't do anything wrong.»

And there were those who were profoundly sceptical towards all sorts of surveillance;

«... even though we have the best intentions about how to use the data (...) It will be misused some day, this is for sure!»

Or;

«All technology can be misused anyway. So there will be persons that try to exploit this.»

1.1 Importance of Technologies

Most of the participants had nuanced views of the dilemmas and consequences of using security technologies. This was also reflected in the evaluation of the statements in the questionnaire. More than 80% of the participants agreed completely or partly with the statement: «The society is absolutely dependent on the development and use of new security technologies». At the other hand almost 80% completely or partly agreed with the statement: «Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror».

1.2 Violation of Privacy

It was a strong perception among the participants that privacy should not be violated. The major part (85%) agreed with the statement: «Privacy should not be violated without reasonable suspicion of criminal intent.»

The discussions indicated that the perception of what violation of privacy is could vary from individual to individual. As one of the participants expressed;

«...people participate voluntarily in «Big Brother». It is a tendency in the society that people don't think it is that important having a private sphere anymore»

Another participant said:

«I could have given a lot of my person to security if I know it works. But if it is protecting criminals, I am not interested!»

This statement illustrates the participants' distrust in criminals and their fear that criminals can take advantage of new security technologies. The major part (87%) agreed with the statement «New security technologies are likely to be abused by criminals».

1.3 Trust in the State

The participants were asked about if they find it probable that governmental agencies will abuse new security technologies. Almost half of the group agreed that this is likely to happen. More than one forth of the group did not know whether they trusted the governmental agencies or not.

There were intense discussions on this topic. Participants who had great trust in the state did not understand the critical viewpoints of participants that expressed distrust towards the state. The first group seemed to believe that the Norwegian state is some kind of a «Big Good Protector». The fact that somebody was questioning this «truth» was disappointing to them and looked upon as some kind of treachery. Below follows some statements that came up during these discussions:

«Don't you have trust in the country?»

«What is the point living in Norway if you cannot trust your own people and your own government?»

Another participant concluded by saying:

«There are Judases everywhere, but not everybody is a Judas.»

1.4 Commercial Interests

There was an outspoken scepticism regarding commercial interests' willingness and possibility to misuse data. As one of the participants expressed;

«... shouldn't it be a limit for what commercial companies are allowed to write in small letters...?»

1.5 Threats

During the discussions most of the groups also touched on the question of what we are protecting ourselves against. What is crime? Is terrorism a real threat in Norway? One participant commented;

«The biggest problem in Norway today is traffic accidents and heart attacks.»

And then the participant suggested to use new security technologies to surveil these threats, for instance by monitoring heart and blood rates for high risk groups.

Another asked;

«What are we going to protect ourselves against? Is it Russia, America, Muslims – it seems that we are going to protect ourselves against each other. I don't want us to protect ourselves against each other!»

And another again;

«There have always been mad persons. How much could you protect yourself against them?»

The last statement was also reflected in several of the discussions. How much freedom must we sacrifice for prevention of a few people's madness? It was said that a major threat for society is to become an intensive surveillance society. Participants questioned if there are other means to fight terrorism and crime, for instance fighting poverty or teaching values to children.

1.6 Significance of Sex, Age and Level of Education

The results from the questionnaire suggest that there is a slight tendency that women are more positive to the use of security technology than men. Men are more doubtful to whether use of security technologies really increases security. Both sexes are concerned about criminals' ability to abuse new security technologies, but women are even more concerned than men.

Age seems to influence the viewpoints. In general the participants above 50 years are slightly more positive to the use of new security technologies and to the effect they can have on the security in society. But even though the trust in new technologies seems to become a bit higher with age, the participants above 50 years are concerned about preserving privacy. 90% of the participants aged 50 or more agreed with the statement «Privacy should not be violated without reasonable suspicion of criminal intent» (compared to 79% of the others).

The participants' level of education seems to have a slight effect on their viewpoints. The participants with higher education were more sceptical about the effects of the use of security technologies and more worried about the possible infringement of privacy and possible abuse of technologies. The participants with lower education are more positive to these issues, but also more uncertain (i.e. they give higher response-rates on «neither agree nor disagree»).

Chapter 2 | Security Technologies

The participants were confronted with specific technologies in the questionnaire, and expressed their attitudes towards the use of these in various situations and conditions. Some of the specific technologies were also debated during the discussions.

2.1 Biometrics

Use of different kinds of biometric technologies was one of the most discussed topics in the group interviews.

About half of the participants reported that they accepted using fingerprints for access control, whereas using facial characteristics was acceptable for only 15% and iris recognition for 35% of the participants. Around 20% of the participants would never use any kind of biometrics. One of them stated;

«For god sake, they could cut your finger off!»

More than half of the participants accepted use of biometrics in border controls (73%) and at airports (54%). Only one fourth accepted use of biometrics in banks. And only a few could accept use of biometrics at sport stadiums and other crowded places (12%), and at central bus and train stations (7%). None of the participants accepted use of biometrics to access stores and other private services.

Even though use of biometrics had the highest degree of acceptance in border control and airports, the predominant part of the participants reported to feel insecure using biometric passports because of the risk of biometric data being stolen (61%).

On the other hand about the same percentage of participants (65%) agreed to storing biometric data of all citizens in a central database to fight crime. One of the participants even expressed:

«Why couldn't it be so that when we were born our DNA was registered? Because if you don't do anything wrong, there is no problem.»

2.2 Camera Surveillance

Viewpoints on camera surveillance were quite divided. About half of the group accepted the use of it in stores, bus and train stations, stadiums and crowded places, and the other half did not. Airports were the kind of location where use of cameras was most accepted (77%), and then banks followed with 65%. Use of camera surveillance in all public places and within dressing rooms was only accepted by a few.

When asked about the number of cameras in public spaces today, a relatively high number (30%) did not know what to answer. This uncertainty was reflected in the group discussions, as the topic of camera surveillance was largely absent.

One participant commented that you might prevent crime with cameras in public places, but then you have to «stand there all day» to be able to be secure.

2.3 Scanning

On the question about where it is necessary to scan persons, the majority of the participants (85%) agreed on airports as such a place, and more than half of the group agreed on public buildings. Participants did mainly not find it necessary to scan persons elsewhere.

On the question about what kind of scanning that is acceptable, luggage scanning was most accepted (73%), but also metal scanning of persons was quite highly accepted (69%), as well as mannequin projection (58%).

Use of «naked-machine» and scanning of body, temperature, sweat and heart had low acceptance rates. As one participant with experience from the «naked machine» said;
«You did really not feel comfortable by passing through.»

2.4 Locating Technologies

In general there seemed to be a low tolerance towards the use of location technologies. This was the situation both regarding location of mobile phones and location of cars. Even with a court order, just about 20% accepted use of location technology to trace cars or mobile phones as a tool for the police.

In emergencies less than 20% found it acceptable to locate cars, and about 60% did not think e-Call should be installed automatically in cars. About 25% of the participants thought it should be possible to deactivate the location technology if installed.

All of the 26 participants were against the use of location technologies for speeding control and automatic speeding tickets. There were also some comments on this issue in the group discussions. As one participant said:

«This must be a joke! (...) to monitor you all the way to see if you exceed the speed limit!»

It was an overall agreement among participants (more than 80%) that locating all cars and all mobile phones is infringing on privacy. At the same time most of the participants agreed that locating a suspect's mobile phone (80%) and car (60%) is a good tool for the police for investigation and prevention of terror and crime.

2.5 Data Retention

Data retention is a topic that received much attention in the discussions, and concerned many of the participants.

More than half of the participants found it acceptable to retain communication data and to scan and combine databases to prevent or investigate crime and terrorism. The acceptance of these kinds of data treatments for commercial use was equal zero.

About half of the participants agreed that governmental institutions could store all the data they find necessary for security reasons. But most of the participants (more than 80%) felt that scanning and combining of governmental databases were privacy infringing and problematic. One participant stated;

«I don't mind collection of data. But what happens to them, and who get access to them is the most important question.»

At the same time about 70% did not think data from phone, mobile and Internet communication should be stored beyond billing.

2.6 Eavesdropping

Eavesdropping for crime and terror prevention and investigation had high acceptance as long as the police has a court order (more than 80%). Only one person did not accept eavesdropping at all, and about 20% accepted it without a court order. This makes this technology one of the most accepted security technologies among the participants. But eavesdropping for commercial purposes was regarded as unacceptable by all 26 participants.

80% thought eavesdropping in general is a serious violation of privacy, but almost the same number of participants thought it is a good tool for the police.

2.7 Privacy Enhancing Technologies

85% of the participants reported that the use of privacy enhancing technologies is necessary in today's society to preserve privacy. But the participants had split viewpoints on which specific technologies should be available for everyone to use. Only about half of the participants evaluated that privacy enhancing technologies as anonymous calling cards, encryption programmes and identity management are acceptable to be legally available for everybody.

The participants were also split in their statements on the question whether privacy enhancing technologies should be illegal if they make police work more difficult (half of the group was positive and the other half was negative to this).

In general there seemed to be some confusion of what PETs are, and which consequences using PETs may have both on an individual level and on a societal level.

2.8 General Attitudes

It is difficult to outline a common attitude to the use of different security technologies among the participants. Almost all technologies mentioned were met with different opinions and viewpoints.

But still there are some general tendencies to be found in the participants' responses.

One tendency is that when a technology or a security practise is familiar, it has a higher acceptance than if it is new or under development. For instance, it is far more accepted to use different security technologies at airports than at any other place. Fingerprints and eavesdropping seem to be quite well accepted for use in police work (with a court order) even though it is looked upon as privacy infringing. These are technologies that have been used in police work for decades.

When it comes to new technologies or new security practises the opinions differs more. During the discussions new security technologies and new possibilities of use were the topics that were the most discussed.

Another finding is that the participants were sceptical towards any kind of locating technologies. The possibility for others tracking your location was evidently looked upon as a violation of privacy.

Also worth mentioning was the clear objections to commercial interests' use of security technologies for commercial purposes. The participants were generally sceptical allowing commercial interests to use security technologies and they were also very sceptical to how commercial companies may infringe our privacy.

Data from the questionnaire was analysed to see if the participants' use of different technologies and travel habits affected their perception of security technologies and privacy. It was not possible to find tendencies illustrating that the participants' use of technologies in their daily life affected their answers. The only tendency that might be worth mentioning concerns the use of privacy enhancing technologies. The people using e-mail and Internet daily seemed to be more positive to use of encryption programmes and identity management than the ones who did not use e-mail and Internet daily. But since the major part of the group used these technologies daily (22 used e-mail and 23 used internet daily out of 26) the numbers cannot be argued to present a significant finding.

Chapter 3 | Dilemmas

In the questionnaire the participants were confronted with various dilemmas concerning privacy and security.

3.1 Convenience When Travelling

The first dilemma the participants were confronted with was whether easier payment in the public transportation system would make them accept using fingerprints as registration. Only a few were willing to accept this privacy infringement for the convenience of easy payment (15%). About a third of the participants would never accept fingerprints used for convenient payment at public transport. The majority indicated that it must be optional to use fingerprint and not the only possibility (60%).

When it comes to travelling by plane the participants were more split in their willingness to accept loss of some degree of privacy for convenience. Almost half of the participants stated that they would accept registration and the use of biometrics for the possibility of using fast-track lines. However, another half stated that they did not accept the use of biometrics and other privacy infringing technologies to improve the efficiency at the airport. Only a few participants would accept going through the «naked-machine» (23%) and being scanned for sweat, body heat and heart rate (12%).

3.2 Prevention of Terror

Active surveillance cameras and automatic face recognition (AFR) in airports and train stations could potentially prevent terrorist attacks, but the participants were not enthusiastic about this technology. About one third of the participants could accept to use the technology if there were no false positives – i.e. nobody will be suspected by mistake. If innocent people would be suspected for being terrorists, only a few participants could accept the use of this kind of cameras. About two thirds of the participants (65%) could accept use of AFR surveillance in exposed locations vulnerable to terror attacks or crime.

Searching and combining data from different databases with personal information in order to detect suspicious patterns are also means in the prevention of terror. When it comes to police searching databases with personal information, most of the participants (65%) accepted this if the data are anonymous and only a court order can have the identity revealed. But at the same time almost one third accepted the police searching and combining all databases to identify patterns that could unveil possible terrorists. About 20% would never accept the police searching and combining data from different databases to search for suspicious patterns.

Some groups discussed if the police and surveillance authorities should be able to decide what kind of security technologies they need and to what extent they should be able to use it. Some participants stated that as long as it prevents crime and terrorism it should be accepted that security solutions are being implemented. Others stated that the needs of governmental surveillance are being created by police, military and governmental institutions. Participants expressed that to prevent that surveillance is used everywhere, there are needed clear rules about what kind of surveillance is accepted and allowed, and what is not.

3.3 Locating Cars and Movements

The e-Call technology can register the movement of cars. This registration can be used for different purposes and with different degrees of privacy infringements. The group of participants expressed deep scepticism about the e-Call system. About two thirds of the participants claimed that installing e-Call should be optional. Nobody agreed to using the e-Call system for giving speeding tickets. About half of the participants meant it should be used only for reporting accidents, and about half meant it could be activated by the police in their work to prevent crime or terrorism.

3.4 Privacy Enhancement for All

Privacy enhancing technologies (PETs) can be used by ordinary people to protect their privacy, e.g. when communicating or using the Internet. But these technologies can also be used by criminals and terrorist, and might make police investigation and prevention of terror and crime more difficult. The opinions about an acceptable legal use of PETs were quite divided. About 40% of the participants did not accept use of PETs if it makes the police work more difficult. At the other hand, about the same number of participants accepted legal anonymous calling cards, legal use of encryption and Internet anonymity even though it might make police investigation and prevention of terror and crime more difficult. One exception was when the participants were questioned about anonymity on the Internet in relation to hindering police' work against child pornography. Only 20% of the participants accepted use of PETs in this situation.

3.5 Consequences for Others

The last dilemma the participants were confronted with was what consequences they would accept for persons that are not able or willing to use security technologies. Consequences could be hinders ore inconveniences with using a service. In general the participants did not tolerate many consequences for people that do not have the possibility to use new technologies. But when asked about people who are not willing to use security solutions, the views were more divided. About half of the participants accepted inconveniences for people that choose not to use the technology. Almost none accepted any exclusion from public services, independent of the reason for their keeping out.

Chapter 4 | Democratic Issues

The participants were asked about their attitudes towards democratic issues like participation and decision making processes as well as proposals for how to handle these topics in the future.

4.1 Democracy and Participation

All participants, except one, thought public debate and public hearings are crucial contributions to decision making when implementing new security technologies. In such open debates it is important that alternative solutions are elucidated and included, stated the majority. Only a minority (20%) agreed that questions about security and privacy are too complicated to involve the general public. As one participant said:

«This is not only something to understand, this is about values.»

The major part of the participants also thought that human rights organisations should be heard when decisions about these topics are to be taken.

The only question that produced divergent meanings on the topic of democracy and participation was whether it is right to include the producers of security technology in the discussions and decision making when developing new technology. Almost one third of the participants completely rejected to include private interests in such a process, and almost one fourth did not know what would be right to do. However, about 50% agreed to include commercial interests in decision making.

This topic was discussed quite a lot in the group. The discussions concerned potential effects of including private companies, such as including as much information as possible into decision making processes. On the other hand, participants recognized the potential dangers of involving private interests, such as that they can corrupt and influence political decisions, with the sole aim to earn more money and with no concern to privacy.

As one of them said;

«...it is important to look at it from their side; if not, the commercial interests will have a hidden agenda.»

Whereas another participant feared that;

«Then they just come and tell us what we kind of surveillance we must implement.»

4.2 Proposals

At the end of the questionnaire the participants were asked to evaluate the importance of four proposals for privacy enhancing use of security technologies. The proposals were evaluated as shown in the following table.

As the table shows all these privacy considerations were regarded as important by the participants.

The two first proposals aim at regulating the use of security technologies. Earlier in this report we have seen that the participants find access to personal data collected by security technologies to be very sensitive. The proposal that only authorized personnel should have access to this data is the one that most participants find to be of most importance. Also the proposal about anonymity until a court order is given is evaluated as important by the participants.

The two other proposals are aiming at the steps prior to implementing new security technology. The proposal about a privacy impact evaluation prior to implementing new technology was given high importance. The proposal on funding of research projects depending on analysis of privacy impacts was also regarded as important. The exceptions were three of the participants that did not know what to answer to this and one that disagreed. The uncertainty by the three could be a result of ignorance about how the research system works as much as not being sure about how privacy impact should be ensured in research.

Proposal	High import.	Some import.	Little import.	Not import.	Don't know
Collection of personal data from unsuspicious individuals must be anonymous until identification is authorised by court order	21	4	1		
Only authorized personnel shall have access to collected personal data	24	2			
Prior to implementing, new security technologies must be checked for privacy impact	21	5			
Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts	15	6		1	3

Chapter 5 | Additional findings

5.1 Participants' Opinions

Security and privacy are complex topics, covering a wide range of uncertainties and ethical dilemmas. The complexity and the sensitivity of these topics were illustrated by participants stating contradictory opinions on the same topic. In other questions some participants were not sure about how to weigh the dilemmas. This is important to take into consideration when reading the results.

It is also a fact that participating in such a meeting, receiving information and being able to discuss the topic with other people might influence the opinions of participants. Only a few participants reported that their opinions had changed in one or another direction (three becoming more sceptical and three becoming less sceptical to the use of new security technologies). But there were also a couple of participants that stated in the discussions that they had become more sceptical to possible privacy infringement of the use of new security technologies, without having reported this in the questionnaire.

5.2 The Norwegian Context

Norwegians are in some ways both geographically and culturally separated from Europe, and this is further enforced by being outside the European Union. The discussions revealed that many of the participants felt more connected to what is going on in the USA than in Europe. This was reflected in the discussions, in two main ways.

1) The participants referred to privacy and security conditions in the USA, rather than to other European countries. The references to the USA regarded both the surveillance conditions and the terror threats. Participants described the situation in the USA as scary and not desirable for Norway. As one participant said:

«Think about me going to the USA. If they scan me, and they find similarities between me and some kind of terrorist, I could risk ending up at Guantanamo for the rest of my life!»

2) Norway was by many referred to as a «different» country. What occurs in the rest of Europe (or the USA), is not necessarily relevant for the situation in Norway. As one commented:

«In this session we have witnessed lots of inspiration from abroad, and Norway as a 'different' country does not always need to follow what others do.»

When the Norwegian context was mentioned by the participants, it always implied that the security situation in Norway is not as serious as in other countries, and that we can accept having a lower level of security than other nations.

Chapter 6 | Annex

6.1 Annex overview

The following is included in the annex (to be found at www.teknologiradet.no):

* Annex 1 – Participants background

* Annex 2 – Program of the interview meeting

* Annex 3 – Material sent to the participants (in Norwegian)

* Annex 4 – Questionnaire and interview guide (in Norwegian)

* Annex 5 – Transcript of group interviews (in Norwegian)

* Annex 6 – Frequency tables

* Annex 7 – Comments from the questionnaire